International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Multi-Biometric Cryptographic Security System with Dynamic Password Protection

Vaibhavkumar Suprao Gaikawad[1], S. N. Kini[2]

[1]M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

[2]Professor (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

Abstract: ***Biometric technologies are used for security purposes by analyzing human characteristics. Unimodal biometric has some limitations which can be overcome with multibiometric. Multibiometric systems also inherits some problems related to the template security. Now a day's network goes on variety of cyber-attacks, and everyone goes for finding a new solution for attacks, it is possible that multibiometric can handle this issue. This Paper presents different types of biometrics attacks and types of multi-model biometric system. Various techniques proposed in developing an authentication system for promising to individual's information security to come together biometric characteristics of that individual and the feature transformations as well as cryptographic techniques. Those problems are difficult for providing a large time security to biometrics. In paper, present a matrix solution method for removing the limitation of current issue and to provide advanced security for individuals as well as groups. Matrix solution method is used with biometrics to map with matrix component and generate the dynamic password as multibiometric for access to system, device or network. A dynamic password which is created is time dependent and generates randomly for user. It provides fundamental idea for research that may help in removing the difficulty associated with the current authentication systems. Biometrics technologies are gaining popularity today since they provide more safe and capable of authentication and verification.***

Keywords: Multi-Biometric, Cryptography, Authentication Accuracy, Dynamic Password, cyber-attacks, Security, Template Protection

1. Introduction

With increasing use of IT technology its necessary to protect stored data, in our daily lives, we have multiple passwords/accounts. We can only remember some of many passwords, so we end up using things we know to create them. It is so easy to crack security passwords, because most of our passwords are related to self and those are weak! If the user creates strong passwords, that should be combinations of different keys, we will forget them! Because is very difficult to remember such passwords. The best solution for this problem is to use bio metrics to protect your devices or accounts. A biometric is a physiologic or behavioral characteristic of a human being that can distinguish between person to person and that can be used for identification or verification of same person identity.

When we decide to use of biometrics then it can be difficult to choose which type is the best for particular work. This is because every biometric has some limitations and benefits. It is not difficult to purloin a biometric of user, create a copy and use the fake trait to attack on biometric systems [6]. This types of problems realizes a requirement of biometric security in network.

Compared with old and traditional authentication techniques such as token cards, token number, picture-based passwords and passwords, biometric-based techniques offer a non-ordinary, more universal and reliable option for personal or group authentication [1]. The system to verify biometric templates consists of the standard universal input-input – match process. The first stage of the above mentioned process is called as the enrolment process. The Second stage is the stage where the new set of data or biometric samples collected again to authenticate the identity of the end user. (Figure 1). It would give the output as match. In the opposite scenario the system may clearly indicate that two users are different or it may raise some concerns or queries or even may ask for more qualitative and or quantitative sample of the data in order to arrive to the conclusion.

Only biometric is not sufficient to provide a security but integrating biometric with the cryptography is to provide a well security. Biometric cryptosystems apply on single biometric (such as face, single fingerprint, iris etc.), limitation of the single biometric cryptosystems (Unimodal) is to provide accuracy and security [1], a multibiometric cryptosystems leads to the theoretical work and practical applications on biometric security. But now a day it is also difficult to provide a security to multiple biometrics because of variety of cyber-attacks.

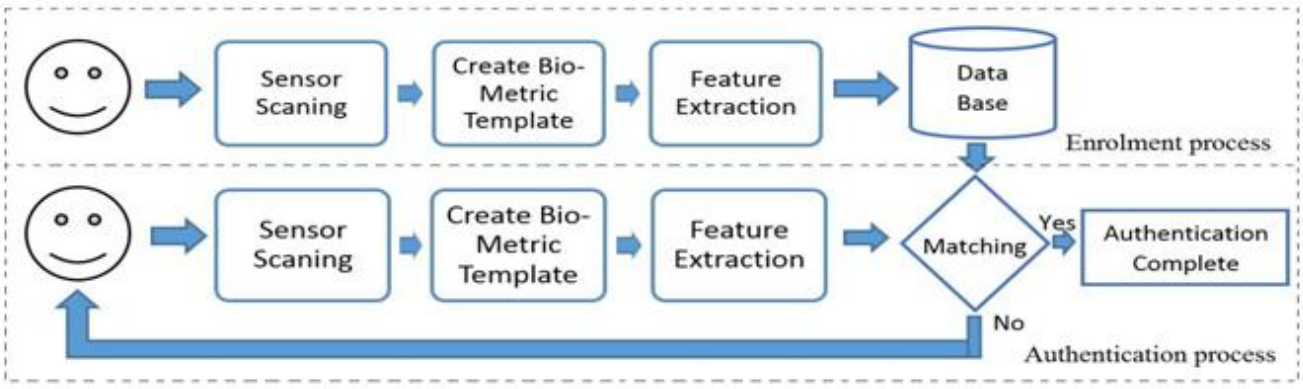

Figure 1: Biometric based authentication system

Matrix solution is method proposed in the paper which is very helpful on the research of biometric security system. It calculates a dynamic password from user's information at the time of enrolment process and provide a security to user's access. Dynamic password is nothing but a password whichcomes at system run time and it depends on time function as expiration time. This password is calculated on system run time that is because it also unknown to the user at the time of authentication session start. Advantage of this password is they are coded in cryptographic format and this is known by only user when he had come for enrolment by using variety of predefined or user defined algorithms and methodologies.

Matrix elements are mapped with user's biometrics that helps to improve a cryptographic security. Also in the paper we present a random matrix which is randomly start them (randomly staring elements) and closed with (randomly end element.)

The rest of the paper is organized as follows: - Section 2 discusses Literature Survey. Section 3 proposes a system includes problem definition, system architecture and mathematical model. Section 4 concentrate on numbers of attacks classes on biometric security and types of multimodal systems also model matrix solution method as example with useful advantage. Section 5 discusses with experimental results.And conclusion is given in section 6.

2. Literature Survey

In [2] biometric based authentication system, overall process can be divides into two processes (1) the enrolment process and (2) the authentication process that helps to understand the functionality of each processing levels. [3] feature transformations (or cancellable biometrics) techniques considered for providing security for template attacks. In that first enroll the data as transformed template is stored for matching and for authentication the transform template is compromised, the system can reissue at next time by a new one using different transformation parameters of the same. [4] Describe a biometric cryptosystem which provide an innovative solution to biometric template protection using cryptographic key generation and encryption. In resents year's researchers concentrate on multibiometric cryptosystems based on feature level fusion (MBCF) because MBCF provides stronger security for single biometric templates and higher recognition accuracy then mu

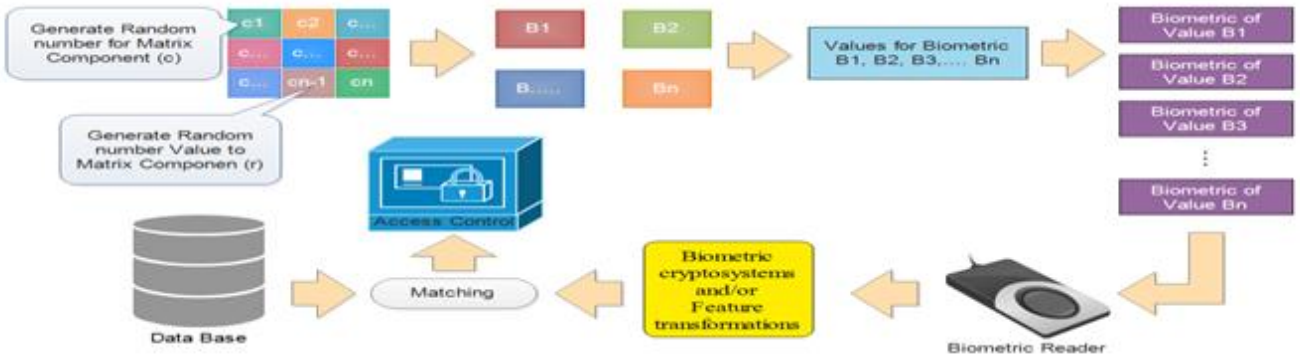

Figure 2: System Architecture

ltibiometric cryptosystems based on decision level fusion (MBCD) [5]. Those both fusions are important in multiple input biometric system. In [6] observe first key binding and second key generating systems are related to the biometric cryptosystems. In [7] analyze the key security, accuracy and template privacy of MBCD (MN-Split model) which use in understanding the providing security on multiple biometrics.

In [8] describe a color pass which is graphics techniques as an intelligent user interface. Color pass is useful to prevent the shoulder surfing attack, hence user can use the session PIN without disclosing the actual PIN. The Color Pass is based on a partially observable attacker model. It also useful for doing work on matrix base password generation technique. And in [9] Dynamic password mechanisms in that mobile the dynamic password scheme is implemented using

Android Operating System, so dynamic password requires a small amount of human computing to secure users passwords. A function/program is used to implement the dynamic password concept. For user-specified functions, we adopt secret little functions and a constant value, in which security is enhanced by hiding both. Here the user only needs to input the system random digits which the system provides and then the dynamic password is automatically calculated for the user.

3. Proposed System

3.1 Problem Definition

Up to the previous work, biometrics basically works only on biometric cryptosystems or feature transformations (cancellable biometrics) but is not sufficient to protect the accounts or system. Multi-biometric cryptographic security system with dynamic password protection discards the limitation of it and to give the more security. There is use a multiple biometric with cryptography as well as feature transformation techniques which can be interact with randomly created time based and dynamic key password which on the same device and same network at only one time. This will be using the matrix solution which is known by the authenticated user only when he going for login account or accessing the device or system on present time. Biometric password use is depending on time function and is dynamic hence they change every time when the user use.

3.2 System Architecture

After successful enrolment of the users we need towards the completion of strong security base authentication process. Figure 2 show the overall structure of secure authentication process. Biometric matrix is logical mapping in between human biometrics and system generated random numbers. A first part of the figure shows a matrix 'M' which divided in two different numbers first is the starting position (location) of the matrix component 'c' (in general Matrix start at M (0,0) position) and second is the inserted value of biometrics 'r' (value for newly find location) (for position c). Using value of r in the looping of component potions c. This first step of the biometric matrix is automatically performing at specific time by randomly generate function.

In second stage figure show B1, B2, B…., and Bn which indicates that are numbers comes out from solving the biometric matrix. For calculating the output of biometric matrix various types of algorithms and methods are defining at the time of user enroll to the system. By using their algorithm or method user can easily calculate or find the solutions. Those outputs of matrix solution can be arranging in first come first serve (FCFS) manner. Solutions for B1, B2, B…., and Bn are in the form of numeric key. This numeric key mapped with user's biometrics in same manners of matrix output comes and that are arranged as biometrics of value B1, biometrics of value B2, biometrics of value B3…...etc. we can simply define that as order of biometrics.

Most important work is to consistently collect and merge multiples biometrics by using biometric readers/scanner with order of biometric. Up to this stage well percent of protection gives to the system, but here next stage used a cryptography and feature transformation techniques for better protection. These techniques used before matching templates stored in database to the current ongoing processes. Advantage of use those techniques before matching are to protect biometrics templates which are possible for permanent loss.

Finally matching process consist of decryption of the encrypted biometric and use matching algorithm to match the authenticated person's biometrics with enroll biometrics of the authorized user. Basically now days the cryptography is good for contradistinguish database attacks and other side the feature transformation is good for template protection. When the user enrolled the all information with their biometrics that all are stored in database. Biometrics templates comes with any one security technology those are matched with database saved template for verification. Finally, the user can be verified by the system it allows for the full system access.

3.3 Mathematical Model

Let M be the matrix,

Their for M = $\begin{bmatrix} M_{00} & \cdots & M_{0b} \\ \vdots & \ddots & \vdots \\ M_{a0} & \cdots & M_{ab} \end{bmatrix}$

This matrix is a (a × b) matrix there are 'a' rows and 'b' columns

1) Calculate or find the starting position (location) of the matrix component 'c',
   This is by using the randomly generated key function which helps to calculate random number. Suppose consider it to rand() function. Here this rand() gives number between 0 and maximum number of biometric used.
2) i.e. int c = rand ();
   Then $M_{a_0 b_0}$ = ?
   a_0 = (c / b) + 1;
   b_0 = (c % b) + 1;
   And increasing it continues up to last component of matrix after again start from zeroth position to $M_{a_0 b_0}$position.
3) int r = rand();
   Again use the same random function to generate the random number this second random number is a value of that component which are located in first random numbers.
4) This is final matrix to be used for biometrics.
5) There are multiples methods to solve this matrix, using specific methods outputs will have mapped with user's biometrics and this sequences of the mapping solution are used for login

4. Implementation Strategy

4.1 Attacks on Biometric Systems

Biometric systems have provided a strong and universally accepted alternatives to traditional token based or password

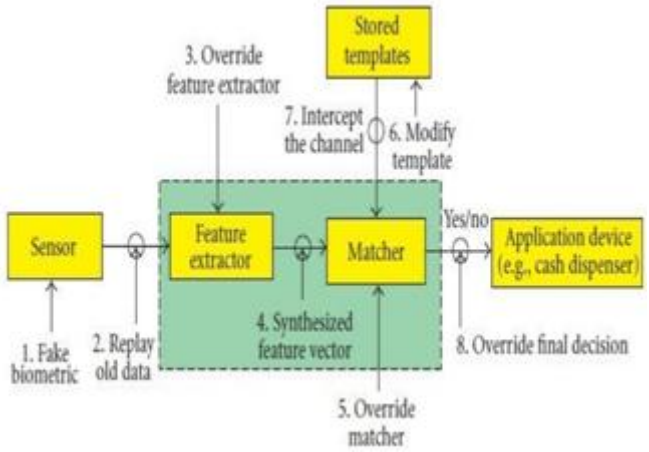

Figure 1: Position of Biometrics Attacks

based identification and access systems along with many advantage over such systems [7]. But the system like its alternative is also not immune to attack and can be compromised There are eight types of attacks that these systems are vulnerable and a point to attacks on network shown in Figure 3. Advantage of this proposed techniques is to protect from all eight types of attacks.

Class I: Spoof attack: this attack is made with the help of and creation fake biometric input given for authentication which is created by copying the original template and (face mask, finger made from silicon, lens including iris texture) can be presents to a sensor [7].

Class II: this attack is known by the name of replay attack. It is possible for an opponent to clarify or acquire a digital copy of the biometric sample which is stored in local database and reply this signal bypassing the biometric sensor.

Class III: Substitution attack: In this type the designer of attack gets access to feature exactor module and replaces it Trojan horse program that functions according to the compromised parameters given by the attacker. Once attacker is successful with the insertion of Trojan horse then he easily gets access to storage either locally or globally. He thus is able overwrite the legitimate user's template (i.e. Replace someone's thumb impression with other person) with his /her own –leading to the stealth of their identity.

Class IV: there are instances when attacker replaces a genuine feature values with other fake values (real or synthetic)

Class V: This class of attack is known as Trojan horse attack. In this Class Trojan horse program is used to replace user matched template.

Class VI: this type of attack targets the template which are saved in database, leading to the template addition, modification or removal in part or complete from the database.

Class VII: This class is called as Transmission attack, also is known as man in the middle attack; Attacker target while the data is transmitted from one component to another in network. The attacker herein compromises the input data stream in-betweens data transmission, create a fake or duplicate template to represent as an authentic enrolled user, can inject an artificial matching perfect score or even may be able to generate a forged response.

Class VIII: Here in the attacker manipulates the result directly instead of template or matcher and be able to manipulate the end results that is match or mismatch.

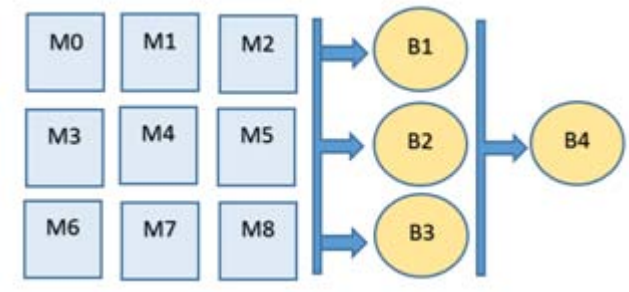

Figure 2: Types of Multimodal Systems

Figure 3: Model Matrix Solution Method

4.2 Types of Multimodal Systems

Multimodal biometric system has few subtypes based on their feature sets, sensor and other parameters. On the basis of the input multimodal system can be classified into basic five types (figure 5). Those are single biometric trait multiple sensors, multiple biometrics, multiple units of single biometric traits, multiple snapshots of single biometric and multiple matching algorithms for the same biometric.

1) Single biometric trait, multiple sensors: In this category multiple sensors use to record the same biometric characteristic to ensure the advanced level of more template security. The raw data collected from different sensors is combined at the feature level or matcher perfect score level thus leading to overall improvement the system performance parameters.

2) Multiple biometrics: In this type multiple biometric traits like as fingerprints (one or combination at given time) and retina are combined and Different sensors are used to map and collect each biometric characteristic data. The system uses interdependency of the traits leading to significant improvement in the performance of the system. For example, a commercial product Bio ID [3] uses multiple biometric traits such as voice tone, lip motion and face of a user to verify his recognition.

3) Multiple units, single biometric traits: When two or more than two fingers of a single user are used as a biometric trait to establish his identity it becomes one of the example of multiple unit's single biometric trait. This system doesn't require multiple sensors on order to extract feature or match modules. Biometric iris can also be included in this category. Due to the same reason is less costly compared to multiple traits biometric even with improved security.

4) Multiple snapshots of single biometric: Best example of this is different emotions on users face. In this category for the recognition, more than one sample of the same biometric trait is used. For example, multiple samples of the voice of the same user are taken to create templates or multiple impressions of the same finger.
5) Multiple matching algorithms for the same biometric: this type of system apply different methods to extract feature and to match the biometric characteristic
All mentions types of multimodal system are used with different fusion modes. Multibiometric cryptosystems are categorized into two based on fusion modes: (1) in the first category the fusion is applied at the feature level (also called as biometric level), and (2) in the second category the fusion is applied at the decision level (also called as cryptographies level) [2].

4.3 Method Implementation

Figure 5 show rectangles that are consider to matrix of 3 rows and 3 columns and circles are the biometric solution of that matrix. First system call generating the random number and allocate that number of component with starting point of the matrix and second generated random number directly allocate to the M_{00} component of the new matrix. By using increment or decrement fill all the remaining components of matrix. This is a final matrix which show to the authorized user. This final matrix looks like as given figure show in that components of matrix are M0 to M8. Biometrics as B1 to B4 are calculate from different mathematical and logical functions that depends on matrix components M0 to M8. When the user enrolls with the system that time only it going to decide which mathematical or logical function to be used for authentication. Suppose that for finding the first biometric value B1 we get a matrix component i.e. M0 and M2 and set one mathematical relation function. Mathematically it can be express as Value (B1) = Mathematical/logical relation (M0, M1 & M2). It is again possible that biometric values relations are not only with matrix components but also indirectly or directly to the others biometrics values. It shows in figure 5 a relation of biometric value B4 with B1, B2 and B3. This is a simple one model to understand method used in matrix solutions and those solutions mapped with user biometrics.

4.4 System Advantage

Multimodal biometric system uses multiple interdependent or weakly correlated biometric template from an individual (e.g., Fingerprint and retina of the same person, or fingerprints from two different fingers of a user) [7]. The major problem in using a single biometric is its insufficient security as well as difficulty in providing sufficient coverage of the user population. Biometric cryptosystems initially applied single biometric (such as iris, face, fingerprints etc.) Their accuracy and security is limited, which has lead to the first theoretical experimental work and then practical applications of multibiometric cryptosystems (MBC). With higher authentication accuracy with security and flexibility in usage, wider coverage and multiple and stronger security layers, multibiometric cryptosystems are rapidly replacing the single biometric cryptosystems.

5. Experimental Results

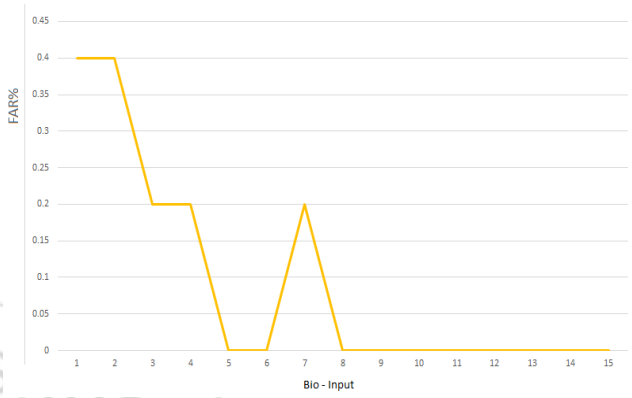

Figure 6: FAR %

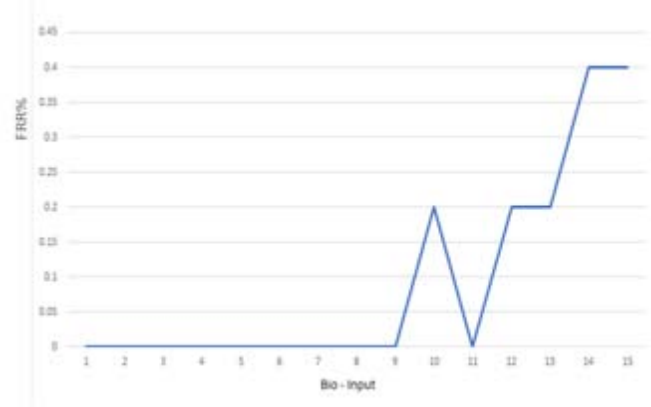

Figure 7: FRR %

There are two major criteria to measure the performanceof a biometric cryptosystem: security and accuracy. To measure the accuracy of biometric cryptosystem we consider the effectiveness of biometric authentication systems, based on False Acceptance Rate (FAR) and False Rejection Rate (FRR).FAR is the probability of an imposter being accepted as anauthorized user, while FRR is the probability of a legitimate user being rejected as an imposter.

In the experiment there are 500 presences with different types of biometrics used. There are 15 biometrics used per person and calculate the FAR and FRR. The results are displayed in figure 6 and figure 7 respectively. It is more clear that the method used for authentication is more secure. The beauty of the experiment is the dynamic password protection. It helps to restrict the unauthorized access. the experimental results conform to the theoretical results with accuracy and security.

6. Conclusion

This paper presents a brief light on multibiometric security systems. At first, we have considered the problems related to

the authentication methods and different passwords security systems and patterns used. We hereby have Also discussed the problems related to the biometric usages and concentrated on how to protect uniqueness of the biometric template from permanent loss. Multibiometric security have a great success over single biometric systems but again they have faced different networks attacks. Proposed methods restricts all the possible cyber-attacks. This paper introduces new multibiometric dynamic security using one-time password by solving the matrix displaying on user's screen which can be encrypted as human identifying cryptographic techniques. Importance of the methods is that encryption used is coded by machine but it is decrypted by human (authenticated) only in given specific time. The existing biometrics systems are used as a limited, static and are for specific purpose but introduced method would be effective to provide stronger security and multipurpose usage.

References

[1] Vaibhavkumar S. Gaikawad, S. N. Kini, "A Survey of Multi-Biometric Cryptographic Security System," International Journal of Science and Research Vol. 4, no.12, pp. 1090 - 1095 December 2015.
[2] Cai Li, Jiankun Hu, Josef Pieprzyk, And Willy Susilo ,"A New Biocryptosystem Oriented Security Analysis Framework And Implementation Of Multibiometric Cryptosystems Based On Decision Level Fusion" IEEE Trans. Information Forensics And Security, Vol. 10, No. 6 Pp. 1193 - 1206, June 2015.
[3] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561 –572, Apr. 2007.
[4] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Proc. Eurocrypt, 2004, pp. 523–540.
[5] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255–268, Feb. 2012.
[6] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–757, Dec. 2007.
[7] Bo Fu, Simon X. Yang, Jianping Li, and Dekun Hu. "Multibiometric Cryptosystem: Model Structure and Performance Analysis," IEEE Transactions on Information Forensics and Security, vol. 4, NO. 4, pp. 867–882, December 2009.
[8] Nilesh Chakraborty and Samrat Mondal, "Color Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack," Proc. IEEE Students' Technology Symposium pp. 1318, 2014
[9] Shimna M S, Sangeetha P S, "Dynamic Password Schemes for Protecting Users from Password Theft for E-Banking," International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-1, June 2013
[10] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinatebased cancelable fingerprint templates," Pattern Recognit., vol. 44, nos. 10–11, pp. 2555–2564, Oct./Nov. 2011.
[11] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," Proc. IEEE, vol. 92, no. 6, pp. 948–960, Jun. 2004.
[12] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 544–560, Apr. 2007
[13] S. Wang and J. Hu, "Alignment-free cancellable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach," Pattern Recognit., vol. 45, no. 12, pp. 4129–4137, Dec. 2012
[14] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templatesfromfingerprint-face features," in *Proc. IEEE Conf. Comput. Vis. PatternRecognit. (CVPR)*, Minneapolis, MN, USA, Jun. 2007, pp. 1–6.

Author Profile

Mr. Vaibhavkumar Suprao. Gaikawad, is pursuing M.E(Computer) from Department of ComputerEngineering, Jayawantrao Sawant College ofEngineering, Pune, India. Savitribai Phule PuneUniversity, Pune, Maharashtra, India -411007. He received his B.E(Computer) Degree from SESCOE Navalnagar, Dhule, India. NorthMaharashtra University, Jalgaon, Maharashtra, India -25001. Hisarea of interest is network Security, Distributed Computing.

Prof. S. N. Kini, received his Ph.D. Degreefrom Cochin University of Science and Technology, Thrikkakara, South Kalamasserry, Cochin. He received hisM.E. (Computer) Degreefrom B.M.S. College of Engineering, Basavanagudi,Bangalore, India. He received his B.E (Computer) Degree from K L E Society's College of EngineeringUdyambaug Belgaum, India. He is currently working as Prof (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His areaof interest is network security and mobile computing.